差分隐私增强的大米区块链品控模型

吴国栋[1,2*], 胡全兴[1,2], 刘　旭[3,4], 秦　辉[1,2], 高博文[1,2]

(1. 安徽农业大学 信息与人工智能学院,安徽合肥 230036,中国; 2. 智慧农业技术与装备安徽省重点实验室,安徽合肥 230036,中国; 3. 中国科学院 成都计算机应用研究所,四川成都 610041,中国; 4. 中国科学院大学,北京 100049,中国)

摘　要: [**目的/意义**] 针对传统大米品质监管追溯系统中存在的品控数据链机制不够完善、品控信息可追溯程度不足、数据上链效率低及隐私信息泄露等问题，提出一种差分隐私增强的大米区块链品控模型。[**方法**] 首先，结合大米全产业链，设计数据传输流程，涵盖种植、收购、加工、仓储和销售等各环节，有效保证品控数据链的连续性；其次，为解决上链数据量大、上链效率低问题，将大米全产业链各环节关键品控数据存储于星际文件系统（InterPlanetary File System, IPFS），然后将存储完成后返回的哈希值上链；最后，为提高品控模型信息可追溯程度，将种植环节关键品控数据中涉及隐私的部分信息通过差分隐私（Differential Privacy）处理后展示给用户，模糊化个体数据，以提高品控信息可信度，同时也保护了农户种植隐私。基于该品控模型，设计了差分隐私增强的大米区块链品控系统，并在相关大米企业实际运行。[**结果与讨论**] 经测试，差分隐私增强的大米区块链品控系统全产业链单环节数据完成存储平均耗时 1.125 s，信息追溯查询平均耗时 0.691 s。与传统大米品质监管追溯系统相比，单环节数据存储时间缩短 6.64%，信息追溯查询时间缩短 16.44%。[**结论**] 研究提出的模型不仅提高了品控数据连续性和信息可追溯程度，同时保护了农户的隐私，还在一定程度上提升了品控数据存储及信息追溯查询的效率，可为大米品质监管与信息追溯系统的设计和改进提供参考。

关键词: 星际文件系统；区块链；品控；高效上链；差分隐私增强；信息追溯

中图分类号: S126;TS272.7　　**文献标志码:** A　　**文章编号:** SA202311027

引用格式:吴国栋, 胡全兴, 刘旭, 秦辉, 高博文. 差分隐私增强的大米区块链品控模型[J]. 智慧农业(中英文), 2024, 6(4): 149-159. DOI：10.12133/j.smartag.SA202311027

WU Guodong, HU Quanxing, LIU Xu, QIN Hui, GAO Bowen. Differential Privacy-enhanced Blockchain-Based Quality Control Model for Rice[J]. Smart Agriculture, 2024, 6(4): 149-159. DOI：10.12133/j.smartag.SA202311027 (in Chinese with English abstract)

0 引　言

大米在日常饮食中扮演着不可或缺的角色。消费者对其质量问题的关注也不断提高，如更加注重选择高品质、安全和健康的大米。但是大米市场存在信息不对称和质量参差不齐等问题，给消费者带来了困扰[1,2]。为满足消费者需求并确保大米质量的可靠性，国内外学者在优化大米供应链、产品信息追溯以及规范大米加工生产过程等方面做了大量研究工作。例如，Qian 等[3] 在大米质量监管和溯源系统方向进行了研究，展现供应链信息与产品溯源之间的关联性；刘陕南等[4]、王莉等[5]、Zhang 等[6] 提出了结合区块链技术提高大米产业体系的数据安全性和可信度的方法。这些研究推动了大米产业的可持续发展。然而，目前大米品质监管追溯系统的研究仍存在不足之处，未充分关注品控与追溯功能之间存在的相互支撑关系。虽然追溯功能可以让产品信息在一定程度上可见，但并不能直接保证产品的质量。通过加强品控措施，不仅可以保证产品质量，还能间接提升追溯功能的可信度[7,8]。传统的大米品质监管追溯系统在品控信息链连续性方面存在缺陷。大米全产业链相关环节信息链不完善甚至缺少重要环节，导致大米品控与溯源信息的可信度大大降低。另外，传统品质监管追溯系统中缺少对稻谷种植相关品控数据的详细统计与展示，

收稿日期：2023-11-15

基金项目：国家自然科学基金（32371993）；安徽省科技重大专项（202103b06020013）；安徽省自然科学基金（2108085MF209）

*通信作者：吴国栋，博士，副教授，研究方向为人工智能、推荐系统。E-mail：8978850@qq.com

导致产品信息可追溯程度不够[9, 10]，其中涉及到的农药使用等信息对大米产品的品质具有重要影响。其次，在大米溯源过程中存在着隐私信息泄露等安全问题，亟待解决[11, 12]。此外，为了确保数据的不可篡改性，常常选择将相关产品的所有信息完全打包上链，从而引发了区块链存储成本较高的问题[13, 14]。

大米产品追溯信息主要来源于全产业链的品控数据，这直接影响到追溯信息的真实性与可靠性。因此，品控对于追溯过程至关重要，同时产品追溯也可作为品控过程的一部分。所以针对当前大米品质监管追溯系统所面临的问题，本研究提出差分隐私增强的大米区块链品控模型，其数据传输流程涵盖种植、收购、加工、仓储及销售等各环节，确保大米质量监管与溯源数据链的连续性。将大米全产业链各环节所需上链的相关数据存储于星际文件系统，返回的星际文件系统（InterPlanetary File System, IPFS）哈希值存储至区块链。通过这种方式，以解决传统数据上链过程中大数据上链成本高的瓶颈问题。为提高大米产品信息的可追溯程度，将采集到的稻谷种植相关数据，包括土壤信息、农用药剂使用等，利用差分隐私技术对其中涉及农户隐私的部分信息进行处理，再将其展示给消费者。品控模型结合大米全产业链，具体剖析并完善数据传输流程，强调大米品控与信息追溯之间存在的相互支撑关系，可靠且连续的品控数据是实现可信追溯的前提，实现可信追溯是大米品控过程的一部分，从大米品控和信息追溯两方面同时出发，为传统大米品质监管追溯系统的优化提供新的解决思路与方案。

1 主要技术

1.1 区块链技术

区块链技术是一种基于密码学和分布式系统的技术，通过分布式共识机制、区块链数据结构和智能合约等关键技术，实现去中心化、不可篡改、透明和安全的数据交换和存储方式[15]。区块链结构如图1所示，其以链式连接区块，保证数据的连续性和完整性[16]。分布式共识机制确保网络中节点对交易的一致性达成共识[17]，智能合约允许在不需要第三方的情况下执行可自动执行的合约逻辑[18]。这使得区块链具备了广泛应用的潜力，可用于金融、供应链管理、医疗保健等领域，为构建信任、提高效率和促进创新提供了新的解决方案[19, 20]。本研究基于区块链技术，提出一种差分隐私增强的大米区块链品控模型，并在以太坊平台（Ethereum）实现该模型的系统化设计与开发。

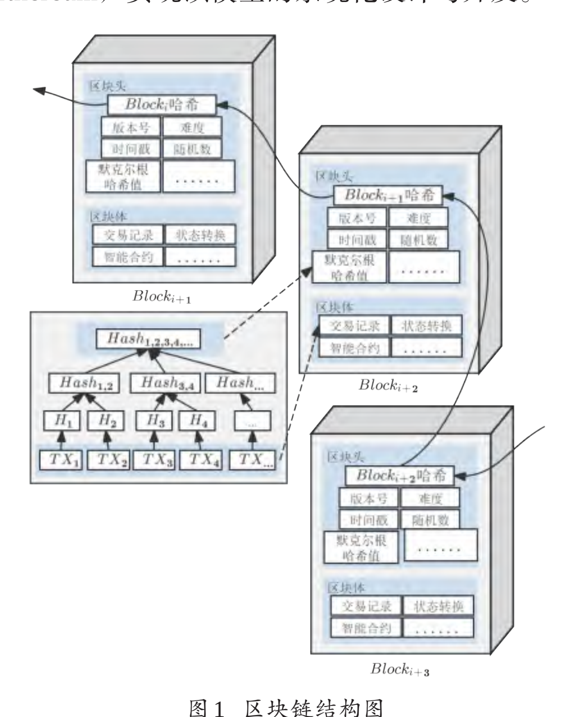


图1 区块链结构图

Fig. 1 Architecture diagram of blockchain

1.2 星际文件系统

IPFS是一种去中心化的分布式文件存储和传输协议，旨在解决传统互联网中的数据存储和传输问题[21]。其存储原理基于内容寻址，使用唯一标识符（Content Identifier, CID）来定位和检索文件。在IPFS中，文件被分割成数据块，并通过哈希函数生成唯一的CID，代表文件内容的哈希，而不是文件的位置，这意味着文件可以通过其内容的唯一标识来定位，而不依赖于特定的服务器或存储位置。IPFS采用分布式哈希表（Distributed Hash Table, DHT）来存储和定位文件块，每个节点都存储一部分哈希表，通过CID在网络中查找包含该CID的节点，并通过分布式协议获取文件块[22]，这种分布式存储机制增加了文件的可用性和冗余性，提高了文件的可靠性和下载速度。

1.3 差分隐私技术

差分隐私是一种隐私保护技术，用于在数据发布或分析过程中保护个体的敏感信息[23]。其通过在查询结果、数据集或算法输出中添加噪声[24]，使得攻击者无法准确推断出个体的敏感信息。差分隐私的数学定义可以表示为：对于任意两个相邻的

数据集D和D'，以及任意查询函数（查询结果的映射）Q，差分隐私要求对于任意输出S，以及任意的隐私攻击者的背景知识K，满足公式（1）。

$$Pr\left[Q(D)\in S\right]\leqslant e^{\varepsilon}\times Pr\left[Q(D')\in S\right] \tag{1}$$

式中：ε为隐私参数，控制噪声的强度，较小的ε值表示更强的隐私保护[25]，但可能导致数据可用性的损失。差分隐私的核心思想是在保护隐私的前提下提供对数据的有用统计分析，通过引入控制噪声的方法，如拉普拉斯噪声或高斯噪声。差分隐私可以实现数据可用性和个体隐私保护之间的平衡[26,27]，它提供数学上的保证，即使在攻击者具有其他背景知识的情况下，也无法从查询结果中还原或推断出个体的敏感信息，通过适当选择隐私参数和噪声添加方式，差分隐私可以在保护个体隐私的同时提供有意义的统计结果。

2　差分隐私增强的大米区块链品控模型

2.1　大米全产业链关键品控数据分析

大米全产业链中包含多个环节，从种植到销售，涉及众多企业的参与和合作。然而，在这些环节之间存在信息孤岛，缺乏有效的品控数据交互，容易导致品质管理和产品追溯的不确定性。因此，建立完整且连续的可追溯环节品控数据链至关重要，不仅有助于确保产品质量稳定，还能提升信息追溯的可信度，为整个产业链的良性发展提供更有力的支持。通过共享、整合数据，各环节可以更加紧密地协作，加强品质管理，提高整体效率，进而增强消费者对产品质量和安全的信心。如表1所示，根据对大米全产业链关键品控数据的分析，按照产业链环节和数据可追溯性进行分类，完成各环节信息上链存储过程后，公开品控数据可直接作为产品追溯信息，种植环节中涉及农户隐私的部分信息进行差分隐私处理后展示，在提高产品信息可追溯程度的同时保护农户的隐私。消费者不可追溯的隐私品控数据，如各环节的成本等，仅限于在相关环节企业内部共享。

表1　大米全产业链关键品控数据

Table 1 Key quality control data of the whole industry chain of rice

全产业链环节	公开可追溯数据	差分隐私处理可追溯数据	不可追溯数据
种植	种植编号、稻谷品种、种植日期、种植地区、土壤类型、施肥量、降水量、灌溉量、光照强度	农药制剂平均用量、土壤碱解氮含量、种植密度	农户信息、种植量、种植成本、利润、灾害损失
收购	收购编号、农户编号、稻谷等级、稻谷名称、收购日期	—	收购量、收购成本、利润
加工	加工编号、加工日期、加工方式、大米等级、打包日期、包装编号、打包方式	—	加工量、出米量、打包量、加工成本、利润
仓储	仓储编号、仓库名称、仓库温度、仓库湿度、入库时间、出库时间	—	仓储数量、仓储成本、利润
销售	订单编号、销售日期、销售用户、产品编号、产品名称、产品批次、产品重量、产品价格、发货编号、发货日期	—	销售成本、销售利润

注：—表示环节数据未经差分隐私处理。

2.2　模型整体架构

基于区块链、星际文件系统等技术，结合差分隐私技术，本研究设计一种具有差分隐私增强的大米区块链品控模型。如图2所示，其核心思想是整合大米全产业链包括种植、收购、加工、仓储和销售等各环节，解决大米产品质量监管和信息追溯中存在的品控数据链不完善问题。另外，通过区块链技术、IPFS技术和差分隐私技术等多种手段，提高大米产品的信息可追溯程度，并同时保证全产业链数据存储与共享效率及隐私安全，实现大米区块链品控模型的全面优化和改进。

模型总体架构可划分为4个层次：物联网设备层、全产业链系统层、IPFS层和区块链层。在物联



图2　差分隐私增强的大米区块链品控模型

Fig. 2 Differential privacy-enhanced blockchain-based quality control model for rice

网设备层，传感器和相关设备在稻谷种植过程收集详细数据，包括湿度、气温、光照以及农药使用等信息，完成关键数据采集后，将其实时上传至云端。全产业链系统层的种植模块存储环节关键品控数据并生成一个唯一的种植信息ID。该ID将作为大米全产业链中信息链的头部。全产业链系统层在整个架构中起到管理和跟踪大米生产过程的作用。它负责存储和管理种植、收购、加工、仓储和销售等环节的相关数据，并构建可靠的信息链以实现大米品控及信息追溯。其中，种植信息ID及相关种植数据将被存储在全产业链系统的种植模块，且在后续的收购、加工、仓储和销售等模块中相应地存储前一环节的唯一编号，从而形成一个可靠的信息链，对大米品控起到关键作用。为解决大量数据上链所带来的开销问题，全产业链各环节在完成数据存储后，通过对应环节IPFS应用程序编程接口（Application Programming Interface, API）将关键品控数据上传至相应的IPFS节点。最后，IPFS返回的哈希值整合存入区块链网络中，完成全产业链环节数据的上链过程。另外，结合差分隐私技术，对种植模块中涉及农户隐私的农药制剂使用等信息进行处理，利用可视化技术将其作为产品追溯信息展示给消费者，同时，施肥量等信息可直接作为产品追溯信息的补充。与物联网设备、全产业链系统、IPFS和区块链层相互协作，构建一个可靠且安全的数据监管与追溯体系，这种架构优化了数据存储和共享的效率，解决大米质量监管与信息追溯中存在的信息链机制不完善及农户隐私泄露问题，同时提高大米产品的信息可追溯性，使消费者能够更加信任和了解所购买的大米产品的来源和品质。

2.3 模型数据流设计

如图3所示，在差分隐私增强的大米区块链品控模型基础上，结合模型中各个层次，完成大米全产业链品控数据流设计。

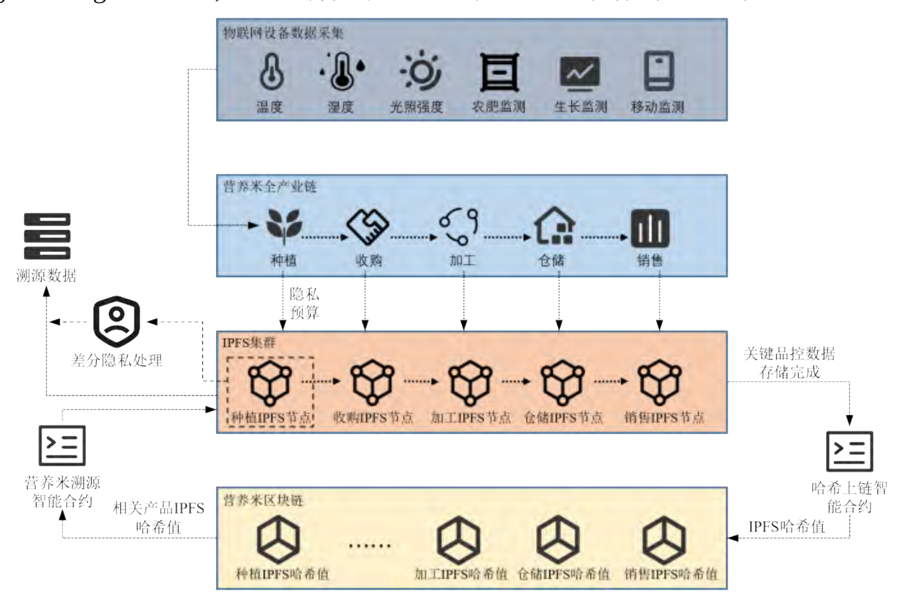


图3 大米全产业链品控数据流

Fig. 3 Quality control data flow of the whole industry chain of rice

物联网设备完成数据完整采集后，将关键品控数据传输至云端，然后存储于大米全产业链系统的种植模块。这包括各类传感器和设备收集的详细种植相关数据，如环境信息等。当大米全产业链系统完成每个环节的信息存储时，关键品控数据将实时上传至相应的IPFS节点，通过将数据进行分块和分布式存储，保证数据的可靠性和持久性，并且允许其他节点快速检索和获取数据。为确保大米全产业链数据的完整性和不可篡改性，将环节数据存储于IPFS返回的哈希值，通过部署在区块链上的哈希上链智能合约进行验证，如哈希编号检验，然后将IPFS哈希值上传至大米联盟链。种植节点、收购节点、加工节点、仓储节点和销售节点在联盟链中代表相关的参与方[28]。在智能合约中，针对种植方、收购方和加工方等不同角色，建立权限控制机制，通过验证节点的身份标识符，限制每个参与方仅能访问和处理与其角色相关的数据。这一设计确保只有经过授权的节点可以访问和处理与其角色相关的数据，从而每个参与方只能访问特定全产业链环节数据，无法获取其他环节的敏感信息，进而

保护数据的隐私和安全。在存储需要进行差分隐私处理的种植溯源数据时，根据种植企业和相关研究机构对一般参数的评估，同时设定隐私预算的预设值。用户追溯大米产品信息时，通过扫描包装二维码或使用大米全产业链系统，基于溯源查询智能合约，验证环节哈希完整性后，获取对应产品的IPFS哈希值，利用该哈希值从IPFS中检索对应的溯源信息，并同时触发差分隐私保护机制。根据预设的隐私预算值，对部分种植数据进行处理，最后再一并返回产品追溯信息。

在该模型数据流设计中，全产业链中的环节关键品控数据相应上传至IPFS，返回哈希值通过哈希上链合约验证后再上传至区块链，保证大米质量监管与追溯数据链连续性的同时，提高数据上链及系统运行的效率。用户进行产品信息追溯时，采用差分隐私处理技术，在部分种植数据中引入噪声，使得个体的隐私信息无法被识别，同时保持数据的整体特性，确保数据的可用性。通过这种方式，保护了农户种植相关的敏感数据，用户仍能够获取深层次的产品追溯信息，在满足用户需求的同时，也避免了农户隐私泄露的问题，进一步提升了品控模型的实用性。

2.4 数据隐私保护设计

为解决传统大米品质监管追溯系统中产品信息可追溯程度不足的问题，品控模型与大米全产业链相结合，能够向用户展示稻谷种植阶段详细的指标统计数据。然而，直接展示的方式可能会导致农户敏感信息的泄露。为此，本研究采用差分隐私技术，在用户追溯查询时对返回的种植溯源数据进行处理，通过对部分数据进行噪声添加，确保农户的隐私个体信息无法被逆向恢复或识别出来。最后，通过可视化技术展示经差分隐私处理后的病虫害防治等信息，以反映数据的分布与变化情况。差分隐私的引入解决了信息追溯中敏感数据展示的难题，为建立更透明的大米品控模型提供了可能性。

具体的种植环节可追溯品控数据差分隐私保护流程，如图4所示。

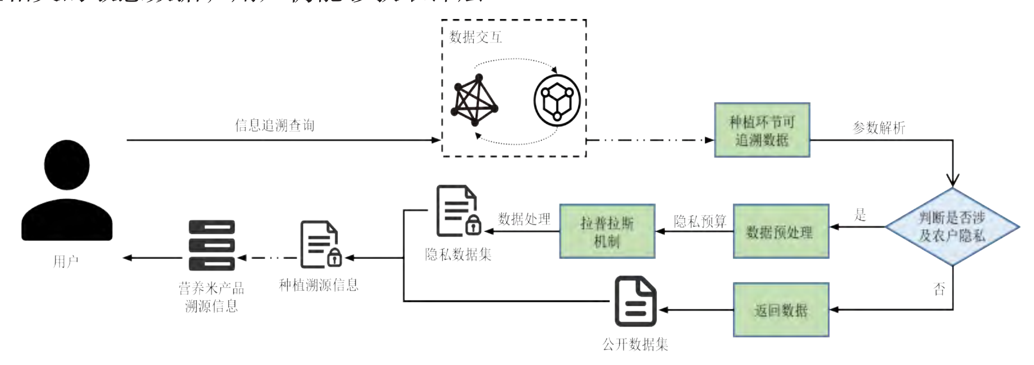


图4 种植溯源数据隐私保护流程

Fig. 4 Privacy protection process for planting traceability data

1）用户进行大米产品信息追溯时，种植环节的部分信息经过差分隐私处理后再统计展示。首先，对种植环节的溯源数据进行参数解析，审查原始数据集的结构和内容，了解数据集的来源、目的；其次，识别数据集中的各个字段，记录字段的名称、含义和数据类型，对于数值型字段，了解其取值范围、单位等信息，对于文本型字段，理解其格式、编码方式等特征；再次，分析字段之间的关系和依赖，了解不同字段之间的关联性；最后，整理并返回参数解析的结果，为后续的差分隐私处理和统计展示奠定基础。

2）若数据集中的字段不涉及农户隐私，则返回原始数据；若数据集中的字段涉及农户隐私，则采用拉普拉斯机制进行差分隐私处理，生成隐私数据集。

3）最后，将经过差分隐私处理的隐私数据集与公开数据集合并，生成隐私保护种植溯源数据集，与其他环节的溯源数据一同返回给用户。

对种植环节可追溯信息的原始数据集进行参数解析之后，使用拉普拉斯机制对数据进行扰动，扰动过程满足ε－差分隐私。具体种植溯源数据差分隐私处理的步骤如下。

1）为确保产品信息的高度可追溯性，对大米进行全面追溯，展示该批次产品所使用稻谷的所有供应农户的种植溯源信息。经过参数解析，得到需要隐私保护的相关数据集。该数据集中包含n个种植农户，记作$P = \{ p_1, p_2, \dots, p_i, \dots, p_n \}$，其中，$p_i$表示第$i$个种植农户，$i$满足$1 \leqslant i \leqslant n$；该批次大

米所用稻谷需要隐私保护的信息有 m 种，记作 $I = \{info_1, info_2, \ldots, info_j, \ldots, info_m\}$，其中，$info_j$ 表示该品种稻谷的第 j 种需要隐私保护的信息，j 满足 $1 \le j \le m$。对于这 n 个供应该批次大米所用品种稻谷的农户，将对该稻谷的 m 种相关种植信息进行隐私保护处理。

2）将第 i 个种植农户 p_i 记录的第 j 种稻谷隐私种植信息表示为 d_{ij}，然后构建一个隐私种植信息矩阵 $\boldsymbol{D}_{n \times m}$。该矩阵包含该批次大米所用稻谷的供应农户记录的可追溯隐私种植信息，其中，n 为农户的数量；m 为该品种稻谷隐私种植信息的类别数量。

3）在隐私保护种植信息矩阵 $\boldsymbol{D}_{n \times m}$ 的基础上，生成一个与其具有相同行数和列数的噪声矩阵 $\boldsymbol{N}_{n \times m}$。当 $\boldsymbol{D}_{n \times m}$ 中的元素 d_{ij} 有效时，第 i 行第 j 列的噪声元素 n_{ij} 服从拉普拉斯分布，满足 $n_{ij} = Laplace(\Delta d/\varepsilon)$，其中，$Laplace()$ 函数为拉普拉斯噪声的随机生成函数[29]；Δd 为全局敏感度，且 $\Delta d = \max(d_{ij}) - \min(d_{ij})$；$\varepsilon$ 为隐私参数，ε 越小代表数据的隐私保护强度越高，但需要根据具体的数据来调整隐私参数的值，以平衡数据的隐私安全性和可用性。

4）在差分隐私中，拉普拉斯分布的概率密度函数满足公式（2）。

$$f(x|e, s) = (1/2s) \times exp\left(-|x - e|/s\right) \tag{2}$$

式中：x 为随机变量；e 为变量 x 的期望；s 为变量 x 的尺度参数；拉普拉斯机制中 $e = 0$，该分布的方差满足 $\sigma^2 = 2s^2$，其中，$s = \Delta d/\varepsilon$。

将噪声矩阵 $\boldsymbol{N}_{n \times m}$ 与种植信息矩阵 $\boldsymbol{D}_{n \times m}$ 相加得到添加噪声后的扰动种植信息矩阵 $\boldsymbol{D}'_{n \times m}$，满足 $\boldsymbol{D}'_{n \times m} = \boldsymbol{D}_{n \times m} + \boldsymbol{N}_{n \times m}$。该扰动种植信息矩阵可被具体表示为公式（3）。

$$\boldsymbol{D}'_{n \times m} = \{d'_{ij} = d_{ij} + n_{ij}, d_{ij} \in \boldsymbol{D}_{n \times m}, n_{ij} \in \boldsymbol{N}_{n \times m}\} \tag{3}$$

扰动种植信息矩阵 $\boldsymbol{D}'_{n \times m}$ 中的第 i 行第 j 列元素 d'_{ij} 满足公式（4）。

$$d'_{ij} = \begin{cases} d_{\min}, d'_{ij} \le d_{\min} \\ d'_{ij}, d_{\min} < d'_{ij} < d_{\max} \\ d_{\max}, d'_{ij} \ge d_{\max} \end{cases} \tag{4}$$

式中：$d_{\max}$ 为种植信息上界；$d_{\min}$ 为种植信息下界，通过限制噪声添加量来提高扰动种植信息的可用性，使数据不会超出原有区间，在保护隐私的同时也一定程度保证数据的可靠性。

上述主要处理步骤可用算法1表示。

算法1：种植溯源数据差分隐私保护

```
输入：敏感溯源数据集 data
      隐私预算 privacy_budget
输出：隐私保护数据 protected_data
Function LaplaceMechanism（data，sensitivity，ε）    //拉普拉斯机制函数
scale ← sensitivity/ε    //计算噪声的尺度
noise ~ Laplace（0.0，scale，size = data.shape）    //生成拉普拉斯噪声
noisy_data ← data + noise    //噪声添加
return noisy_data
End Function
Function ApplyDifferentialPrivacy（data，ε）
param_values ← ExtractParameterValues（data）    //数据处理
sensitivity ← Max（param_values，axis=0）-Min（param_values，axis=0）    //计算敏感度
noisy_param_values = LaplaceMechanism（param_values，sensitivity，ε）    //拉普拉斯机制
data ← noisy_param_values
return data
End Function
Original data example：
  data ←
```

'粳稻'	zhang**	li*	liu*	xu*	zhang*
农药制剂用量 $(g(mL)/667m^2)$	375.63	350.25	386.34	323.22	315.89
土壤碱解氮含量 (mg/kg)	173.52	178.55	157.43	180.23	165.43
种植密度(万穴 $/hm^2$)	16.20	17.55	14.70	16.70	15.10

```
privacy_budget ← 0.5
Function ApplyDifferentialPrivacyWithBudget（data，privacy_budget）
protected data ← ApplyDifferentialPrivacy（data.copy( )，privacy_budget）
return protected data
End Function
```

3 系统设计与实现

3.1 系统总体结构设计

基于品控模型，设计差分隐私增强的大米区块链品控系统，其架构如图5所示。系统架构根据具体功能可被划分为物理层、传输层、存储层、服务层和应用层。其中，物理层作为系统架构的底层，涉及传感器设备和网络基础设施，负责确保全产业链各环节相关数据的采集，包括温度、湿度以及气体浓度等数据，为上层提供可靠的数据基础；传输层负责数据的传输和通信，利用各种通信协议和技术，包括互联网、局域网和蓝牙等，将从物理层采集到的数据上传至云端，并对数据进行加密和压缩，以确保数据传送过程中的安全性和高效性；存储层由传统数据库、IPFS和区块链组成，通过它们的协同作用，实现系统关键数据在区块链上与链下

的高效存储和管理。传统数据库用于结构化数据的管理和查询，IPFS存储全产业链环节中的关键品控数据，而区块链则用于IPFS返回哈希值的存储。这种综合存储方式提高了系统的运行效率，并保证了大米系统中品控数据链的连续性、可靠性和可追溯性，为消费者提供了可信赖的大米品控信息；服务层在系统架构中承担着重要任务，主要负责处理业务逻辑和提供功能服务，包括接收用户请求、进行数据验证和授权等。应用层的功能实现主要依赖于服务层中一系列API设计来完成；系统架构的最上层是应用层，负责提供面向用户的功能和界面，涵盖Web应用程序、移动应用程序等，用于系统的数据展示与功能交互，以满足质检认证、用户和产品管理、大米产品销售、大米产品信息追溯和部门监管等多种需求。

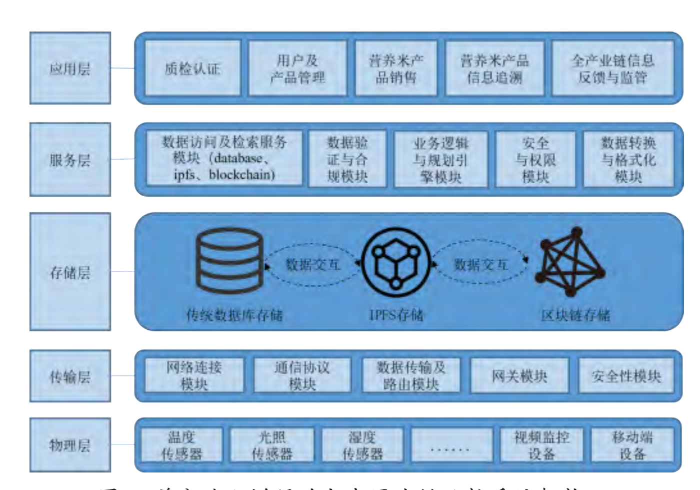


图5　差分隐私增强的大米区块链品控系统架构

Fig. 5 Architecture of differential privacy-enhanced blockchain-based quality control system for rice

3.2　系统实现

基于上述系统架构的设计，本研究实现了差分隐私增强的大米区块链品控系统，并在安徽省六安市相关大米企业得到实际应用，有效解决了大米企业及传统大米全产业链中存在的品控数据存储连续性不足、上链效率低、产品信息可追溯程度不够以及农户隐私泄露等问题。在大米全产业链各环节中，需要大量的物联网设备来收集并实时上传信息，以确保产业链的安全和高效运行。图6展示了系统物理层中所使用的部分物联网设备。图6a为粮情测控分机，用于实时监测大米仓库或储存设施中的温度、湿度、气体浓度等参数，并根据这些数据进行智能控制和调节，以确保大米的安全储存和保持良好的品质；图6b为大米加工监测台，在大米加工过程中，可以监测并控制大米加工的实时步骤与状态；图6c为粮食重金属分析仪，用于检测和分析大米中的重金属含量。





a.粮情测控分机



b.大米加工监测台



c.粮食重金属分析仪

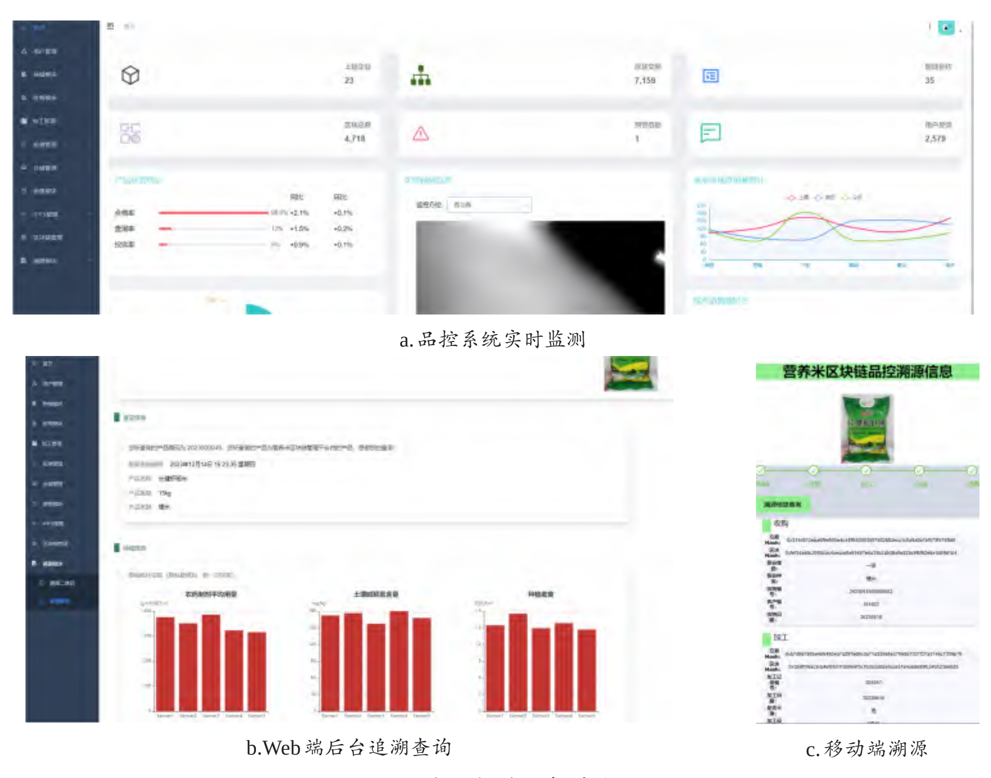
图6　大米品控系统的物理层相关物联网设备

Fig. 6 Physical layer related IoT devices of quality control system for rice

系统架构中的底层为应用层提供必要的基础设施和功能服务，以支持上层应用运行，实现特定的业务需求。图7展示了部分系统相关应用。图7a为品控系统后台的监测主页，可以显示实时监测区块链相关信息，如上链企业、区块交易、智能合约和区块总数等。此外，还能查看销售客户端反馈的实时数据。通过这些功能，企业可以实现对全产业链各环节的全面管理和监测。图7b为Web端后台信息追溯查询页面，便于企业检验和追溯相关大米品控信息，获取大米全产业链各环节的关键信息。其中，种植环节中的部分溯源信息经过差分隐私处理，最终以统计视图形式将数据呈现给消费者。图7c为移动端的溯源页面，消费者可以通过大米包装编号或二维码进行产品信息追溯，展示了包括种植、收购、加工、仓储和销售等大米全产业链各环节的溯源信息，与Web端后台追溯查询信息一致。

3.3　系统测试与分析

本系统基于以太坊客户端Geth v1.12.1完成开发，采用工作量证明（Proof of Work, POW）机制，编写语言包括Java、Solidity和Javascript。采用阿里云服务器与线下实体服务器结合的方式部署系统，依托实体服务器所处的堡垒机保护环境，搭建用于项目访问的内部网络。通过这种架构，充分利



a.品控系统实时监测

b.Web端后台追溯查询　　c.移动端溯源

图7　大米品控系统相关应用

Fig. 7 Applications related to quality control system for rice

用阿里云服务器的弹性和灵活性，同时借助实体服务器的安全性和稳定性。在具体配置方面，阿里云服务器采用8核64 GB硬件配置，带宽为20 Mbps，使用Ubuntu 20.04 LTS操作系统，以更好地支持Docker容器化技术和其他开源技术。此外，内网采用Zerotier技术，将阿里云服务器和实体服务器虚拟网络连接起来，实现安全的内网连接。

在产品信息追溯过程中，引入差分隐私保护机制防止农户隐私泄露，然而对查询性能会造成一定影响。为验证差分隐私增强的大米区块链品控系统，在结合差分隐私技术实现系统产品信息可追溯程度安全提高的同时，是否也保证大米全产业链环节数据存储及追溯查询的效率，测试全产业链包括种植、收购、加工、仓储和销售各环节的关键品控数据存储所需时间及产品信息追溯查询所需的时长。

为确保实验结果的严谨性与真实性，与传统区块链存储和查询型大米区块链品质监管追溯模型做出对比，各进行200次全产业链环节数据存储效率测试及200次产品信息追溯查询效率测试。在具体实验中，测试数据选用六安市企业某种大米产品的全产业链各环节关键品控数据。改进方法存储过程包括将关键品控数据存入传统数据库、按模块上传至IPFS和环节哈希值存入大米区块链，每次存储包含58条品控参数信息；溯源查询结果为关键品控数据中的可追溯数据，每次查询包含40条品控参数信息，其中敏感溯源信息经过差分隐私处理。在传统模型中，关键品控数据直接从传统数据库上传至区块链，完成存储测试；在追溯查询测试中，隐私溯源数据作为一般溯源参数可视化展示，从而与改进模型进行定量对比。每20次测试的结果取平均值作为一个数据点，如图8所示，改进方法系统全产业链环节数据完成存储平均耗时5.623 s，其中，单个环节存储平均耗时1.125 s；传统单链存储方法环节数据完成存储平均耗时6.025 s，单个环节存储平均耗时1.205 s；改进方法单环节存储用时相比减少6.64%。由此可以看出用IPFS哈希值上链代替数据直接上链，可以较好解决大数据上链引起的时延问题。如图9所示，在引入差分隐私算法的情况下，改进方法大米产品信息追溯查询平均耗时0.691 s；传统方法大米信息追溯查询平均耗时0.827 s；改进方法信息追溯查询用时相比减少16.44%。由此可见，结合区块链和IPFS进行溯源的方法，可以较好地弥补大米品控模型中差分隐私处理过程所带来的查询性能损耗，且在一定程度上提高了信息追溯查询的效率，印证了差分隐私保护

机制在大米品控模型中的适用性。

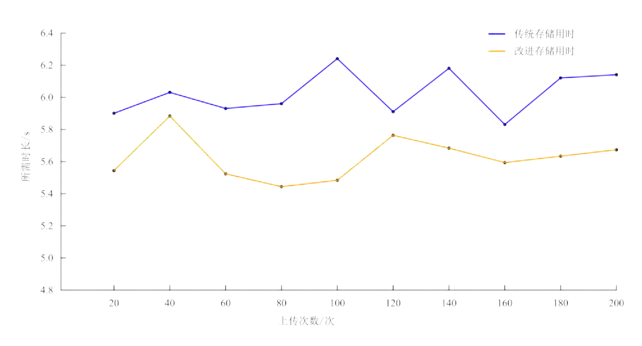


图8　大米品控系统的全产业链环节数据存储测试

Fig. 8 Test of system-wide industry chain data storage of quality control system for rice

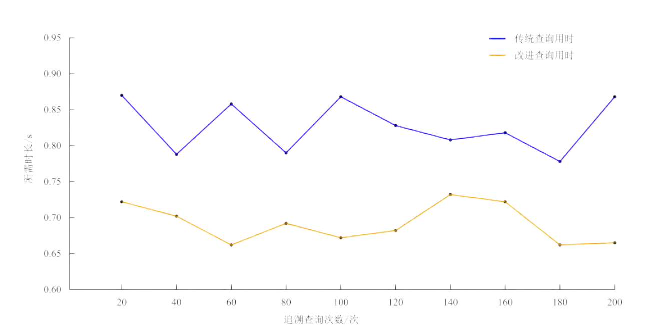


图9　大米产品信息追溯查询测试

Fig. 9 Test of rice product information traceability query

4　结　论

针对传统大米品质监管追溯系统中存在的品控信息链机制不完善、品控信息可追溯程度不足、数据上链效率低与隐私泄露等问题，本研究提出一种差分隐私增强的大米区块链品控模型。结合大米全产业链，设计了数据传输流程，包含种植、收购、加工、仓储、销售等各环节，有效保证了品控数据链的连续性。在此基础之上，采用区块链结合IPFS存储模式解决了传统上链中数据量大和效率低等问题。最后，为了提高品控模型的产品信息可追溯程度，将部分敏感的稻谷种植环节数据通过差分隐私保护处理，利用可视化技术统计信息后展示给用户，在提高产品信息可追溯程度的同时保护了农户个人的种植隐私。

基于品控模型，设计了差分隐私增强的大米区块链品控系统，通过在相关大米企业的实际运行，表明本系统不仅能提高大米品控信息连续性与信息可追溯程度，还有效保护了农户的隐私。在大米关键品控数据存储和信息追溯查询效率方面，系统全产业链单环节数据完成存储平均耗时1.125 s，信息追溯查询平均耗时0.691 s，与传统大米区块链品质监管追溯模型相比，单环节数据存储时间缩短6.64%，信息追溯查询时间缩短16.44%，也取得了较好的效果，可为大米全产业链品控系统的设计与改进提供参考。

利益冲突声明：本研究不存在研究者以及与公开研究成果有关的利益冲突。

参考文献:

[1] TAO Q, CAI Z Y, CUI X H. A technological quality control system for rice supply Chain[J]. Food and energy security, 2023, 12(2): ID e382.

[2] 张全意, 李太平. 中国大米质量安全研究[J]. 粮食与油脂, 2022, 35(11): 143-146.
ZHANG Q Y, LI T P. Study on the rice and safety in China[J]. Cereals & oils, 2022, 35(11): 143-146.

[3] QIAN L L, ZUO F, ZHANG C D, et al. Geographical origin traceability of rice: A study on the effect of processing precision on index elements[J]. Food science and technology research, 2019, 25(5): 619-624.

[4] 刘陕南, 刘长征, 张荣华, 等. 基于区块链智能合约的有机大米追溯研究[J]. 中国农机化学报, 2024, 45(1): 217-222, 251.
LIU S N, LIU C Z, ZHANG R H, et al. Research on organic rice traceability based on blockchain smart contract[J]. Journal of chinese agricultural mechanization, 2024, 45(1): 217-222, 251.

[5] 王莉, 任健荣, 王涛, 等. 基于区块链的粮食防伪溯源系统的设计与实现[J]. 科学技术与工程, 2023, 23(4): 1625-1634.
WANG L, REN J R, WANG T, et al. Design and implementation of food security traceability system based on blockchain[J]. Science technology and engineering, 2023, 23(4): 1625-1634.

[6] ZHANG Y, WU X Y, GE H Y, et al. A blockchain-based traceability model for grain and oil food supply chain[J]. Foods, 2023, 12(17): ID 3235.

[7] 卞立平, 吕滢, 罗智彬, 等. 基于区块链技术的食品溯源在元宇宙中的应用构想与设计[J]. 智能化农业装备学报(中英文), 2023, 4(4): 11-19.
BIAN L P, LYU Y, LUO Z B, et al. Application conception and design of food traceability in the Metaverse based on blockchain technology[J]. Journal of intelligent agricultural mechanization, 2023, 4(4): 11-19.

[8] 梁昊, 刘思辰, 张一诺, 等. 面向农产品交易流程的多链式区块链应用技术研究[J]. 智慧农业, 2019, 1(4): 72-82.
LIANG H, LIU S C, ZHANG Y N, et al. Multi-blockchain application technology for agricultural products transaction[J]. Smart agriculture, 2019, 1(4): 72-82.

[9] 高阳阳, 吕相文, 袁柳等. 基于区块链的农产品安全可信溯源应用研究[J]. 计算机应用与软件, 2020, 37(7): 324-328.
GAO Y Y, LYU X W, Y L, et al. Application of blockchain-based trusted traceability of agricultural products[J]. Computer applications and software, 2020, 37(7): 324-328.

[10] 王敏学, 李波, 温书凝, 等. 区块链技术赋能食品供应链溯源综述分析[J]. 电子科技大学学报(社科版), 2023, 25

(2): 42-54.
WANG M X, LI B, WEN S N, et al. Reviewing analysis on traceability in food supply chain empowered by blockchain technology[J]. Journal of UESTC (social sciences edition), 2023, 25(2): 42-54.
[11] 李天明, 严翔, 张增年, 等. 区块链+物联网在农产品溯源中的应用研究[J]. 计算机工程与应用, 2021, 57(23): 50-60.
LI T M, YAN X, ZHANG Z N, et al. Application research of blockchain+internet of things in agricultural product traceability[J]. Computer engineering and applications, 2021, 57(23): 50-60.
[12] 查凯金, 王志波, 何月顺, 等. 区块链安全保护研究综述[J]. 计算机与现代化, 2023(6): 110-117.
ZHA K J, WANG Z B, HE Y S, et al. Survey on blockchain security protection[J]. Computer and modernization, 2023(6): 110-117.
[13] SINGH A, GUTUB A, NAYYAR A, et al. Redefining food safety traceability system through blockchain: Findings, challenges and open issues[J]. Multimedia tools and applications, 2023, 82(14): 21243-21277.
[14] 司冰茹, 肖江, 刘存扬, 等. 区块链网络综述[J]. 软件学报, 2024, 35(2): 773-799.
SI B R, XIAO J, LIU C Y, et al. Survey on blockchain network[J]. Journal of software, 2024, 35(2): 773-799.
[15] GUO H Q, YU X J. A survey on blockchain technology and its security[J]. Blockchain: Research and applications, 2022, 3(2): ID 100067.
[16] FAN X, NIU B N, LIU Z L. Scalable blockchain storage systems: Research progress and models[J]. Computing, 2022, 104(6): 1497-1524.
[17] WANG X Y, YIN S R. Research on Database Storage Technology based on Consensus Mechanism[C]// Proceedings of the 2nd International Conference on Bigdata Blockchain and Economy Management. Hangzhou, China: EAI, 2023.
[18] PENG X Z, ZHAO Z Y, WANG X Y, et al. A review on blockchain smart contracts in the agri-food industry: Current state, application challenges and future trends[J]. Computers and electronics in agriculture, 2023, 208: ID 107776.
[19] ZHAO Y D, LI Q D, YI W L, et al. Agricultural IoT data storage optimization and information security method based on blockchain[J]. Agriculture, 2023, 13(2): ID 274.
[20] BALCERZAK A P, NICA E, ROGALSKA E, et al. Blockchain technology and smart contracts in decentralized governance systems[J]. Administrative sciences, 2022, 12(3): ID 96.
[21] ATHANERE S, THAKUR R. Blockchain based hierarchical semi-decentralized approach using IPFS for secure and efficient data sharing[J]. Journal of king Saud university-computer and information sciences, 2022, 34(4): 1523-1534.
[22] 陈泓达, 冯云霞, 牛云鹤. 基于IPFS区块链技术的工业互联网数据可信存储系统[J]. 计算机科学与应用, 2022, 12: ID 1292.
CHEN H D, FENG Y X, NIU Y H. Industrial internet data trusted storage system based on IPFS blockchain technology[J]. Computer science and application, 2022, 12: ID 1292.
[23] 王腾, 霍峥, 黄亚鑫, 等. 联邦学习中的隐私保护技术研究综述[J]. 计算机应用, 2023, 43(2): 437-449.
WANG T, HUO Z, HUANG Y X, et al. Review on privacy-preserving technologies in federated learning[J]. Journal of computer applications, 2023, 43(2): 437-449.
[24] WU X T, QI L Y, GAO J Q, et al. An ensemble of random decision trees with local differential privacy in edge computing[J]. Neurocomputing, 2022, 485: 181-195.
[25] ADNAN M, KALRA S, CRESSWELL J C, et al. Federated learning and differential privacy for medical image analysis[J]. Scientific reports, 2022, 12: ID 1953.
[26] SARKAR A, SHARMA A, GILL A, et al. A differential privacy-based system for efficiently protecting data privacy[C]// 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS). Piscataway, New Jersey, USA: IEEE, 2023: 1399-1404.
[27] VASA J, THAKKAR A. Deep learning: Differential privacy preservation in the era of big data[J]. Journal of computer information systems, 2023, 63(3): 608-631.
[28] LI J T, HAN D Z, WU Z D, et al. A novel system for medical equipment supply chain traceability based on alliance chain and attribute and role access control[J]. Future generation computer systems, 2023, 142(C): 195-211.
[29] WU Q T, LI M W, ZHU J L, et al. DP-RBAdaBound: A differentially private randomized block-coordinate adaptive gradient algorithm for training deep neural networks[J]. Expert systems with applications, 2023, 211: ID 118574.

Differential Privacy-enhanced Blockchain-Based Quality Control Model for Rice

WU Guodong[1,2*], HU Quanxing[1,2], LIU Xu[3,4], QIN Hui[1,2], GAO Bowen[1,2]

(1. *College of Information and Artificial Intelligence, Anhui Agricultural University, Hefei* 230036, *China*; 2. *Anhui Provincial Key Laboratory of Smart Agriculture Technology and Equipment, Hefei* 230036, *China*; 3. *Chengdu Institute of Computer Application, Chinese Academy of Sciences, Chengdu* 610041, *China*; 4. *University of Chinese Academy of Sciences, Beijing* 100049, *China*)

Abstract:

[Objective] Rice plays a crucial role in daily diet. The rice industry involves numerous links, from paddy planting to the consumer's ta-

ble, and the integrity of the quality control data chain directly affects the credibility of rice quality control and traceability information. The process of rice traceability also faces security issues, such as the leakage of privacy information, which need immediate solutions. Additionally, the previous practice of uploading all information onto the blockchain leads to high storage costs and low system efficiency. To address these problems, this study proposed a differential privacy-enhanced blockchain-based quality control model for rice, providing new ideas and solutions to optimize the traditional quality regulation and traceability system.

[Methods] By exploring technologies of blockchain, interplanetary file system (IPFS), and incorporating differential privacy techniques, a blockchain-based quality control model for rice with differential privacy enhancement was constructed. Firstly, the data transmission process was designed to cover the whole industry chain of rice, including cultivation, acquisition, processing, warehousing, and sales. Each module stored the relevant data and a unique number from the previous link, forming a reliable information chain and ensuring the continuity of the data chain for quality control. Secondly, to address the issue of large data volume and low efficiency of blockchain storage, the key quality control data of each link in the rice industry chain was stored in the IPFS. Subsequently, the hash value of the stored data was returned and recorded on the blockchain. Lastly, to enhance the traceability of the quality control model information, the sensitive information in the key quality control data related to the cultivation process was presented to users after undergoing differential privacy processing. Individual data was obfuscated to increase the credibility of the quality control information while also protecting the privacy of farmers' cultivation practices. Based on this model, a differential privacy-enhanced blockchain-based quality control system for rice was designed.

[Results and Discussions] The architecture of the differential privacy-enhanced blockchain-based quality control system for rice consisted of the physical layer, transport layer, storage layer, service layer, and application layer. The physical layer included sensor devices and network infrastructure, ensuring data collection from all links of the industry chain. The transport layer handled data transmission and communication, securely uploading collected data to the cloud. The storage layer utilized a combination of traditional databases, IPFS, and blockchain to efficiently store and manage key data on and off the blockchain. The traditional database was used for the management and querying of structured data. IPFS stored the key quality control data in the whole industry chain, while blockchain was employed to store the hash values returned by IPFS. This integrated storage method improved system efficiency, ensured the continuity, reliability, and traceability of quality control data, and provided consumers with reliable information. The service layer was primarily responsible for handling business logic and providing functional services. The implementation of functions in the application layer relied heavily on the design of a series of interfaces within the service layer. Positioned at the top of the system architecture, the application layer was responsible for providing user-centric functionality and interfaces. This encompassed a range of applications such as web applications and mobile applications, aiming to present data and facilitate interactive features to fulfill the requirements of both consumers and businesses. Based on the conducted tests, the average time required for storing data in a single link of the whole industry chain within the system was 1.125 s. The average time consumed for information traceability query was recorded as 0.691 s. Compared to conventional rice quality regulation and traceability systems, the proposed system demonstrated a reduction of 6.64% in the storage time of single-link data and a decrease of 16.44% in the time required to perform information traceability query.

[Conclusions] This study proposes a differential privacy-enhanced blockchain-based quality control model for rice. The model ensures the continuity of the quality control data chain by integrating the various links of the whole industry chain of rice. By combining blockchain with IPFS storage, the model addresses the challenges of large data volume and low efficiency of blockchain storage in traditional systems. Furthermore, the model incorporates differential privacy protection to enhance traceability while safeguarding the privacy of individual farmers. This study can provide reference for the design and improvement of rice quality regulation and traceability systems.

Key words: IPFS; blockchain; quality control; efficient on-chain; differential privacy enhancement; information traceability

Foundation items: National Natural Science Foundation of China (32371993); Anhui Provincial Major Science and Technology Project (202103b06020013); Anhui Provincial Natural Science Foundation (2108085MF209)

***Corresponding author:** WU Guodong, E-mail: 8978850@qq.com